Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] What is claimed is:

1.A method for implementing advanced encryption standards (AES) by using a very long instruction word (VLIW) architecture processor, the processor comprising:

a buffer for storing data;

a first register electrically connected to the buffer having a plurality of output ports and a plurality of input ports;

an input/output (I/O) controller electrically connected to the buffer and the first register for controlling data to be transmitted from the first register to the buffer or from the buffer to the first register;

an arithmetic logic unit (ALU) comprising:

a plurality of input ports;

a plurality of output ports;

a basic logic operation unit for executing basic logic operations; and

a special AES command unit for executing special logic operations according to AES;

a plurality of multiplexers each having a plurality of input ports electrically connected to the output port of the first register or the output port of the ALU, and one output port electrically connected to the output port of the

ALU and the output port of the first register;
a command input port for receiving commands of AES execution;
a command register electrically connected to the command input port for temporarily storing the commands input to the command input port; and
a command decoder/scheduler electrically connected to the command register, the plurality of multiplexers, and the ALU for decoding and scheduling the commands from the command register in order to control at least one of the multiplexers to output and input one of the plurality of data units stored in the multiplexer to the ALU and control the ALU to operate,
the method comprising:
(a)inputting the command of AES execution into the command input port;
(b)sending the command stored in the command input port to the command register;
(c)sending the command input into the command register to the command decoder/scheduler;
(d)decoding and scheduling the command sent from the command register to the command decoder/scheduler;
(e)controlling at least one of the multiplexers to output one of the plurality of data units input into the multiplexer from the first register and the ALU to the ALU and the first register, and controlling the ALU to operate; and

(f)inputting data generated by the operation of the ALU into the plurality of multiplexers.

[c2] 2.The method of claim 1, being able to process and execute commands for a plurality of different modes according to AES.

[c3] 3.The method of claim 1, being able to execute 128-bit, 192-bit, 256-bit AES (AES-128, AES-192, AES-256) encryption/decryption.

[c4] 4.The method of claim 1, wherein the first register comprises a plurality of registers including register R0, register R1, register R2 and register R3, and the method is able to execute an SBSR1 (substitute byte shift row 1) command and simultaneously process the least significant byte (LSB) and the second least significant byte counted for 8 bytes stored in register R0, register R1, register R2, register R3.

[c5] 5.The method of claim 4, being able to execute an SBSR2 command and simultaneously process the most significant byte (MSB) and the second most significant byte counted for 8 bytes stored in register R0, register R1, register R2, and register R3.

[c6] 6.The method of claim 1, wherein the first register comprises a plurality of registers including register R0, reg-

ister R1, register R2 and register R3, and the method is able to execute an MIXADK1 (mix column add round key 1) command and simultaneously process data stored in register R0 and register R1.

[c7] 7.The method of claim 6, being able to execute an MIX-ADK2 command and simultaneously process data stored in register R2 and register R3.

[c8] 8.The method of claim 1, being able to simultaneously generate an AES encryption key and encrypt a plain text according to AES.

[c9] 9.The method of claim 1, being able to simultaneously generate an AES encryption key and encrypt a plurality of plain texts according to AES.

[c10] 10.The method of claim 1, wherein the first register comprises a plurality of registers including register R0, register R1, register R2, and register R3, and the method is able to execute an INVSBSR1 (inverse substitute byte shift row 1) command and simultaneously process the LSB and the second least significant byte counted for 8 bytes stored in register R0, register R1, register R2, and register R3.

[c11] 11.The method of claim 10, being able to execute an IN-VSBSR2 command and simultaneously process the MSB

and the second most significant byte counted for 8 bytes stored in register R0, register R1, register R2, and register R3.

[c12] 12.The method of claim 1, wherein the first register comprises a plurality of registers including register R0, register R1, register R2 and register R3, and the method is able to execute an INVMIXADK1 (inverse mix column add round key 1) command and simultaneously process data stored in register R0 and register R1.

[c13] 13.The method of claim 12, being able to execute an INVMIXADK2 command and simultaneously process data stored in register R2 and register R3.

[c14] 14.The method of claim 1, wherein the first register comprises a plurality of registers including register R20, register R21, register R22 and register R23, and the method is able to execute an SBSR3 command and simultaneously process the LSB and the second least significant byte counted for 8 bytes stored in register R20, register R21, register R22, and register R23.

[c15] 15.The method of claim 14, being able to execute an SBSR4 command and simultaneously process the MSB and the second most significant byte counted for 8 bytes stored in register R20, register R21, register R22, and

register R23.

[c16] 16.The method of claim 1, wherein the first register comprises a plurality of registers including register R20, register R21, register R22 and register R23, and the method is able to execute an MIXADK3 command and simultaneously process data stored in register R20 and register R21.

[c17] 17.The method of claim 16, being able to execute an MIXADK4 command and simultaneously process data stored in register R22 and register R23.

[c18] 18.The method of claim 1, wherein the first register comprises a plurality of registers including register R20, register R21, register R22 and register R23, and the method is able to execute an INVSBSR3 command and simultaneously process the LSB and the second least significant byte counted for 8 bytes stored in register R20, register R21, register R22, and register R23.

[c19] 19.The method of claim 18, being able to execute an INVSBSR4 command and simultaneously process the MSB and the second most significant byte counted for 8 bytes stored in register R20, register R21, register R22, and register R23.

[c20] 20.The method of claim 1, being able to execute AES en-

cryption/decryption in OCB (offset code book) mode and CCM (counter mode with CBC MAC) mode.

[c21] 21.The method of claim 1, being able to use the same encryption key to simultaneously encrypt a plurality of data units.